Factorization of $Q(h(T)(x))$ over a Finite Field Where $Q(x)$ is Irreducible and $h(T)(x)$ is Linear—I

Andrew F. Long

and

Theresa P. Vaughan
Department of Mathematics
The University of North Carolina at Greensboro
Greensboro, North Carolina 27412

Submitted by Alston S. Householder

ABSTRACT

Let GF(q) be the finite field of order q, let $Q(x)$ be an irreducible polynomial in GF(q)(x), and let $h(T)(x)$ be a linear polynomial in GF(q)[x], where $T: x \to x^q$. We use properties of the linear operator $h(T)$ to give conditions for $Q(h(T)(x))$ to have a root of arbitrary degree k over GF(q), and we describe how to count the irreducible factors of $Q(h(T)(x))$ of degree k over GF(q). In addition we compare our results with those of Ore which count the number of irreducible factors belonging to a linear polynomial having index k.

1. INTRODUCTION

Let GF(q) denote the finite field of order $q = p^k$, where p is prime and k is a positive integer. Throughout this paper, $Q(x)$ will denote an irreducible polynomial of degree n over GF(q), where for convenience we always assume that $Q(x)$ is monic.

Long has considered the factorization of $Q(x^{q^r} - x)$ in [4]. In this paper, we use different techniques to generalize the results of [4] to the factorization of $Q(h(T)(x))$, where $h(x) = \sum_{i=0}^{r} a_i x^i$, $a_i \in \mathrm{GF}(q)$, and $T: x \to x^q$.

O. Ore in [5] has classified the irreducible factors of $Q(h(T)(x))$ over GF(q) according to the unique linear polynominal $L(T)(x)$ to which such a factor belongs. [The polynomial $\phi(x)$ belongs to the linear polynomial $L(T)(x)$ if and only if $L(x)$ is the polynomial of least degree for which $\phi(x)$ divides $L(T)(x)$.] Ore gives the number of irreducible factors of $Q(h(T)(x))$ over GF (q) which belong to $L(T)(x)$.

In this paper we classify the irreducible factors of $Q(h(T)(x)$ over GF(q) according to degree, and we give the number of irreducible factors of each degree. Our main results, given in Sec. 4, may be summarized as follows:

Let α be any root of $Q(x)$. Let N be any positive integer, and let $\ker h(T)$ denote the kernel of the linear transformation $h(T)$ of GF(q^N) over GF(q). Suppose that $(h(x), x^N - 1) = d(x)$, where the degree of $d(x)$ is j. Then, if $h(T)(x) - \alpha$ has a root in GF(q^N), we have $N = nk$ for some positive integer k, and the number of roots of $h(T)(x) - \alpha$ in GF(q^N) is given by

$$M_N = |\ker h(T)| = q^j.$$

If $h(T)(x) - \alpha$ has no roots in GF(q^N), we put $M_N = 0$.

For each positive integer k, define R_{nk} to be the number of roots of $h(T)(x) - \alpha$ of degree exactly nk. Thus

$$M_{nk} = \sum_{k'|k} R_{nk'}$$

and, by the Möbius inversion formula,

$$R_{nk} = \sum_{k'|k} \mu\left(\frac{k}{k'}\right) M_{nk'}$$

where μ is the Möbius μ-function. Then the number of irreducible factors of $Q(h(T)(x))$ of degree nk over GF(q) is

$$N_{nk} = \frac{R_{nk}}{k}.$$

The classification of irreducible factors given by Ore in [5] is finer than the classification by degree which we give in this paper. On the other hand, Ore's classification requires much more information about the polynomials $Q(x)$ and $h(x)$ than is necessary for the classification by degree. In Sec. 5, we illustrate the computational difference in Example 5.1.

The factorizations for the examples included in this paper were obtained by Professor J. T. B. Beard, Jr. and Karen I. West of the University of Texas at Arlington, using computer programs which they have recently developed [1]. We gratefully acknowledge their assistance.

2. SOME PRELIMINARY CONCEPTS AND THEOREMS

Most of these results are found in [2], [4], [5], and [6]. The definitions and results due to Ore are first stated in their original formulation, and then they are restated in terms of linear transformations.

DEFINITION 2.1. If α is contained in $\mathrm{GF}(q^s)$ but is not contained in $\mathrm{GF}(q^t)$, $1 \leqslant t < s$, then s is called the *degree of* α *relative to* $\mathrm{GF}(q)$.

We use the notation $\deg \alpha = s$.

DEFINITION 2.2. A polynomial of the form

$$F(x) = \sum_{i=0}^{s} a_i x^{q^i}$$

is called a *linear* polynomial [5].

DEFINITION 2.3. Let $F(x)$ and $G(x)$ be linear polynomials. The *symbolic product* $F \times G$ is given by

$$F \times G(x) = F(G(x)).$$

In general the symbolic product is not commutative, but it is commutative if the a_i of Definition 2.2 belong to $\mathrm{GF}(q)$.

DEFINITION 2.4. The linear polynomial

$$F(x) = \sum_{i=0}^{s} a_i x^{q^i}$$

is said to *correspond* to the ordinary polynomial

$$f(x) = \sum_{i=0}^{s} a_i x^i.$$

DEFINITION 2.5. In Definition 2.4, the degree s of $f(x)$ is called the *order* of $F(x)$.

DEFINITION 2.6. If $F(x)$ is a linear polynomial with smallest order divisible by the polynomial $\phi(x)$, we say that $\phi(x)$ *belongs to* $F(x)$.

THEOREM 2.1. *Every polynomial $\phi(x)$ of degree s belongs to a unique linear polynomial $F(x)$ with order $t \leqslant s$.*

THEOREM 2.2. *For each linear polynomial $F(x)$ without repeated roots there exists a smallest number n such that*

$$x^{q^n} - x = G(x) \times F(x).$$

DEFINITION 2.7. In Theorem 2.2, n is called the *index* of $F(x)$.

Every irreducible ordinary factor of $F(x)$ has a degree dividing the index n.

THEOREM 2.3. *An irreducible polynomial of degree n belongs to a linear polynomial with index n, and conversely, every irreducible polynomial belonging to a linear polynomial with index n has degree n.*

For comparison with the results of this paper we quote the following theorem of Ore [5, p. 253]:

THEOREM 2.4. *Let $\phi_1(x)$ be an irreducible polynomial over* GF(q) *of degree N_1, belonging to the linear polynomial $F_1(x)$; let $F_2(x)$ be a second linear polynomial and*

$$F_1(x) = G_1(x) \times D_1(x),$$

$$F_2(x) = G_2(x) \times D_2(x),$$

where $D_1(x)$ and $D_2(x)$ contain the prime factors common to $F_1(x)$ and $F_2(x)$. The polynomial $\phi_1(F_2(x))$ is then equal to a product of irreducibles over GF(q) *belonging to the linear polynomials*

$$\bar{D}(x) \times D_2(x) \times F_1(x), \tag{2.1}$$

where $\bar{D}(x)$ is any divisor of $G_2(x)$. The number of irreducibles belonging to each of the polynomials in (2.1) *is*

$$\frac{N_1}{\bar{N}} q^{d_2} \Phi\big(\bar{d}(x)\big)$$

where $\bar{N}$ is the index of (2.1), *d_2 the exponent of $D_2(x)$, $\bar{d}(x)$ the polynomial corresponding to $\bar{D}(x)$, and $\Phi(x)$ the Euler Φ-function.*

It will be convenient to introduce a notation different from that used by Ore.

We consider the finite field $\mathrm{GF}(q^n)$ as an n-dimensional vector space over $\mathrm{GF}(q)$. The map $T: x \to x^q$ is then a linear transformation of $\mathrm{GF}(q^n)$. Let $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ be any polynomial with coefficients in $\mathrm{GF}(q)$. The linear polynomial $F(x)$ corresponding to $f(x)$ is

$$F(x) = a_0 x + a_1 x^q + \cdots + a_k x^{q^k},$$

and it is clear that we may identify $F(x)$ with the linear transformation $f(T)$. We shall write

$$F(x) = f(T)(x).$$

It is also clear that the set of roots of $F(x)$ in $\mathrm{GF}(q^n)$ is precisely the kernel of $f(T)$, which as usual is denoted by $\ker f(T)$.

We shall require some properties of the linear transformation T, which we state here without proof (for a detailed discussion, see [6]).

THEOREM 2.8. *The linear transformation $T: x \to x^q$ of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$ has minimum and characteristic polynomials both equal to $x^n - 1$.*

COROLLARY 2.1. *Let T be the linear transformation of Theorem* 2.8. *If $x^n - 1 = f(x)\,g(x)$, then $\ker f(T)$ is a T-invariant subspace of $\mathrm{GF}(q^n)$, and the minimum polynomial of T restricted to $\ker f(T)$ is $f(x)$. Also, $\ker f(T)$ = range of $g(T)$. Conversely, if W is a T-invariant subspace of $\mathrm{GF}(q^n)$ and if $h(x)$ is the minimum polynomial of T restricted to W, then $h(x) \mid x^n - 1$, say $h(x)k(x) = x^n - 1$, and $W = \ker h(T)$ = range of $k(T)$.*

THEOREM 2.9. *Let $Q(x)$ be an irreducible polynomial of degree n over $\mathrm{GF}(q)$. Thus $Q(x)$ has n roots, say $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, in $\mathrm{GF}(q^n)$. Let W be the T-invariant subspace of $\mathrm{GF}(q^n)$ generated by the roots of $Q(x)$. Then $Q(x)$ belongs to $f(T)(x)$ (in the sense of Ore) if and only if $W = \ker f(T)$ and $f(x)$ is the minimum polynomial of T restricted to W.*

3. SOME PRELIMINARY LEMMAS

LEMMA 3.1. *Let $h(x) \in \mathrm{GF}(q)[x]$. Then $h(T)(x)$ has no repeated roots if and only if $h(0) \neq 0$.*

Proof. We have

$$h(T)(x)=\sum_{i=0}^{k} a_i x^{q^i},$$

and so the derivative of $h(T)(x)$ is just $h(0)$. If $h(0)\neq 0$, it follows that $h(T)(x)$ has no repeated roots. On the other hand, if $h(0)=0$, we have for some $j>0$,

$$h(x)=\sum_{i=j}^{k} a_i x^i \qquad (a_j\neq 0).$$

Then

$$h(T)(x)=\sum_{i=j}^{k} a_i x^{q^i}=\left[\sum_{i=0}^{k-j} a_{i+j} x^{q^i}\right]^{q^j}=\left[h_1(T)(x)\right]^{q^j}, \tag{3.1}$$

and the distinct roots of $h_1(T)(x)$ have multiplicity q^j for $h(T)(x)$. ■

LEMMA 3.2. *Let $Q(x)$ be irreducible of degree n over $\mathrm{GF}(q)$, and suppose that $Q(x)$ belongs to $f(T)(x)$. Then $f(T)(x)$ has no repeated roots.*

Proof. By Theorem 2.9 and Corollary 2.1, we have that $f(x)|x^n-1$. Thus $f(0)\neq 0$, and Lemma 3.1 applies. ■

LEMMA 3.3. *Let $f(x),g(x)\in \mathrm{GF}(q)[x]$. If $f(T)(x)$ and $g(T)(x)$ have no repeated roots, then $f(T)\,g(T)(x)$ has no repeated roots.*

Proof. From the hypothesis and Lemma 3.1 it follows that $f(0)\neq 0$ and $g(0)\neq 0$. Now the product $(fg)(x)$ satisfies

$$(fg)(0)=f(0)\,g(0)\neq 0,$$

and the result follows from Lemma 3.1. ■

4. THE FACTORIZATION OF $Q(h(T)(x))$

In this section we prove various results which, taken together, will allow the determination of the degrees of the irreducible factors of $Q(h(T)(x))$

and the number of irreducible factors of each degree. To facilitate concise statements of the theorems we list the hypotheses on $Q(x)$ as follows:

CONDITION A. Let $Q(x)$ be an irreducible polynomial of degree n over $GF(q)$, and let $f(T)(x)$ denote the linear polynomial to which $Q(x)$ belongs. Also let α of degree n over $GF(q)$ be determined by the factorization

$$Q(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i})$$

in $GF(q^n)$.

In the following discussion we assume that $h(x)$ is a polynomial over $GF(q)$ with $h(0) \neq 0$. Then, according to Lemma 3.1, $h(T)(x)$ will have no repeated roots. This assumption can be made without loss of generality. For if $h(0) = 0$, then (3.1) shows that the distinct root of $h_1(T)(x)$ are repeated q^i times in $h(T)(x)$. Allowing repeated roots will not affect the work which follows, except to multiply the counts of roots and irreducible factors of $Q(h(T)(x))$ by q^i.

LEMMA 4.1. *Let $h(x) \in GF(q)[x]$. Let N be any integer and suppose that $(h(x), x^N - 1) = d(x)$. Let W_1 [W_2] be the range of the linear transformation $h(T)$ [$d(T)$] in $GF(q^N)$ over $GF(q)$, and let V_1 [V_2] be the kernel of $h(T)$ [$d(T)$] in $GF(q^N)$ over $GF(q)$. Then $W_1 = W_2$ and $V_1 = V_2$.*

Proof. Since $(h(x), x^N - 1) = d(x)$, we may write $h(x) = d(x)k(x)$ and $x^N - 1 = d(x)\bar{d}(x)$. From Corollary 2.1, we have $W_2 = \ker \bar{d}(T)$.

It is well known that if $f(x)$ is any polynomial over $GF(q)$ with $(f(x), \bar{d}(x)) = 1$, then $f(T)$ is non-singular on W_2. Clearly $(k(x), \bar{d}(x)) = 1$; hence $k(T)$ is a non-singular (one to one) linear operator on W_2. Now

$$h(T)(x) = k(T)d(T)(x). \tag{4.1}$$

We observe that as x runs through the elements of $GF(q^N)$, the right member of (4.1) takes on all values of W_2 [since the range of $d(T)(x)$ is W_2, and $k(T)$ is one to one on W_2]. The left member of (4.1) takes on all values of W_1; hence $W_1 = W_2$.

Since $d(x) | h(x)$, it is clear that $V_2 \subseteq V_1$. But $\dim V_1 + \dim W_1 = N = \dim V_2 + \dim W_2$ implies that $\dim V_1 = \dim V_2$. Thus $V_1 = V_2$. ∎

THEOREM 4.1. *Let Condition A be given. Let N be an integer divisible by n, and let*

$$\big(h(x), x^N - 1\big) = d(x),$$

$$h(x) = d(x)k(x),$$

$$x^N - 1 = d(x)\bar{d}(x).$$

Then $h(T)(x) - \alpha$ has a root in $\mathrm{GF}(q^N)$ if and only if $Q(x)$ divides $\bar{d}(T)(x)$, hence if and only if $f(x)$ divides $\bar{d}(x)$.

Proof. Since N is divisible by n, it follows that $\alpha \in \mathrm{GF}(q^N)$. By Lemma 4.1, if W_1 and W_2 are the ranges in $\mathrm{GF}(q^N)$ of $h(T)$ and $d(T)$ respectively, then $W_1 = W_2$. As before, we also have

$$W_2 = \ker \bar{d}(T)$$

where $\bar{d}(x)$ is the minimum polynomial of $T|W_2$. If $\alpha \in \ker \bar{d}(T)$, then $\alpha^{q^i} \in \ker \bar{d}(T)$ $(i = 0, 1, \ldots, n-1)$ since $\ker \bar{d}(T)$ is a T-invariant subspace of $\mathrm{GF}(q^N)$. On the other hand, $\ker \bar{d}(T)$ is just the set of roots of the polynomial $\bar{d}(T)(x)$, and thus $\alpha \in \ker \bar{d}(T)$ if and only if $Q(x) | \bar{d}(T)(x)$. Since $Q(x)$ belongs to $f(T)(x)$, it must also be that $\alpha \in \ker \bar{d}(T)$ if and only if $f(x) | \bar{d}(x)$. Since $\ker \bar{d}(T)$ is equal to the range of $h(T)$ in $\mathrm{GF}(q^N)$ by Lemma 4.1 and Corollary 2.1, the result follows. ∎

THEOREM 4.2. *Let Condition A be given. Let N be any integer, and let $\ker h(T)$ be the kernel of the linear transformation $h(T)$ of $\mathrm{GF}(q^N)$ over $\mathrm{GF}(q)$. If $h(T)(x) - \alpha$ has a root in $\mathrm{GF}(q^N)$, then $n | N$, and the number of roots of $h(T)(x) - \alpha$ of degree dividing N is given by*

$$M_N = |\ker h(T)|.$$

Proof. Suppose $h(T)(\gamma) - \alpha = 0$, where $\deg \gamma$ divides N. Now $\alpha = h(T)(\gamma)$ implies that $\deg \alpha | \deg \gamma$. Since $\deg \alpha = n$, we have $n | N$.

If $h(T)(x) - \alpha$ has one root in $\mathrm{GF}(q^N)$, then [since $h(T)$ is a linear transformation of $\mathrm{GF}(q^N)$ over $\mathrm{GF}(q)$] the set of roots of $h(T)(x) - \alpha$ in $\mathrm{GF}(q^N)$ is a coset of $\ker h(T)$ in $\mathrm{GF}(q^N)$. The cardinality of such a coset is

$$M_N = |\ker h(T)|.$$

This proves Theorem 4.2. ∎

COROLLARY 4.1. *Let Condition A be given. Let N be any integer divisible by n, and suppose that $h(T)(x)-\alpha$ has a root in $\mathrm{GF}(q^N)$. Let*

$$\big(h(x),x^N-1\big)=d(x),$$

where the degree of $d(x)$ is j. Then

$$M_N=q^j.$$

Proof. By Corollary 2.1, the minimum polynomial of T restricted to $\ker d(T)$ is $d(x)$. By Lemma 4.1, $\ker d(T)=\ker h(T)$ in $\mathrm{GF}(q^N)$. Hence the dimension of $\ker h(T)$ is j, the degree of $d(x)$. Since $\ker h(T)$ is thus a subspace of dimension j over $\mathrm{GF}(q)$, we have $M_N=|\ker h(T)|=q^j$. ∎

DEFINITION 4.1. Under Condition A, for each integer $N>0$ we define the quantity M_N to be 0 if $h(T)(x)-\alpha$ has no roots of degree dividing N. Otherwise, M_N is given by Theorem 4.2.

REMARK. In view of Theorem 4.2, it is clear that if $h(T)(x)-\alpha$ has a root of degree N, then $N=nk$ for some positive integer k.

THEOREM 4.3. *Let Condition A be given. For each integer $k>0$, let R_{nk} denote the number of roots of $h(T)(x)-\alpha$ of degree exactly nk. Then*

$$R_{nk}=\sum_{k'|k}\mu\Big(\frac{k}{k'}\Big)M_{nk'}, \tag{4.2}$$

where $\mu(j)$ is the Möbius μ-function. Let N_{nk} denote the number of irreducible factors of $Q(h(T)(x))$ of degree nk over $\mathrm{GF}(q)$. Then

$$N_{nk}=\frac{R_{nk}}{k}. \tag{4.3}$$

Proof. From the definitions of M_{nk} and R_{nk} we have

$$M_{nk}=\sum_{k'|k}R_{nk'}. \tag{4.4}$$

We obtain (4.2) from (4.4) by applying the Möbius inversion formula.

Since

$$Q(x)=\prod_{i=0}^{n-1}(x-\alpha^{q^i}),$$

we have

$$Q(h(T)(x))=\prod_{i=0}^{n-1}\left[h(T)(x)-\alpha^{q^i}\right].$$

We observe first that γ is a root of $h(T)(x)-\alpha$ of degree nk if and only if γ^{q^i} is a root of $h(T)(x)-\alpha^{q^i}$ of degree nk. Secondly, if γ is a root of $h(T)(x)-\alpha$ of degree nk, then

$$\prod_{i=0}^{nk-1}(x-\gamma^{q^i})$$

is a factor of degree nk of $Q(h(T)(x))$ which is irreducible over GF(q). Thus the number of irreducible factors of degree nk is

$$N_{nk}=\frac{nR_{nk}}{nk}=\frac{R_{nk}}{k}.$$

■

5. SOME EXAMPLES AND A COMPARISON WITH THE RESULTS OF ORE

In our first example we compare our results directly with those of Ore.

Let GF(q), $Q(x)$, and $h(x)$ be given as in Sec. 4, with $Q(x)$ belonging to $f(T)(x)$ and

$$Q(x)=\prod_{i=0}^{n-1}(x-\alpha^{q^i}).$$

Suppose that

$$f(x)=g_1(x)d_1(x),$$

$$h(x)=g_2(x)d_2(x), \tag{5.1}$$

where $(g_1(x), g_2(x)) = 1$ and $d_1(x)$ and $d_2(x)$ contain all (and only) the common factors of $f(x)$ and $h(x)$ in GF$(q)[x]$. Put

$$D = \left\{ t(x) = \frac{g_2(x)}{r(x)} d_2(x) f(x) : r(x) \mid g_2(x) \right\}.$$

O. Ore has shown in [4] that $Q(h(T)(x))$ has a factor of degree k if and only if k is the index of $t(T)(x)$ for some $t(x)$ in D. [Lemma 3.2 and 3.3 insure the existence of the index for each $t(T)(x)$ in D.] In addition Ore shows that every irreducible factor of $Q(h(T)(x))$ over GF(q) belongs to $t(T)(x)$ for some $t(x)$ in D, and for each $t(x)$ in D, Ore gives the number of irreducible factors of $Q(h(T)(x))$ belonging to $t(T)(x)$.

In contrast, the results of Sec. 4 give the number of irreducible factors of $Q(h(T)(x))$ of a given degree k. In view of the fact that there is no general method of deciding which and how many of the polynomials $t(x)$ in D have the index of $t(T)(x)$ equal to a given integer k, it is clear that the results of Ore and the results in Sec. 4 are qualitatively different. To illustrate, we give the following example:

EXAMPLE 5.1. $Q(x) = x + 1$, which is irreducible over GF(3). $Q(x)$ belongs to $f(T)(x) = x^3 - x$, so that $f(x) = x - 1$. Let $h(x) = x^3 + x^2 + x + 1$. Then

$$Q(h(T)(x)) = x^{3^3} + x^{3^2} + x^3 + x + 1.$$

Beard [1] has given the factorization of $Q(h(T)(x))$ to be

$$Q(h(T)(x)) = (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 + 2x + 2)(x^4 + x^3 + 2)$$

$$\times (x^4 + x^3 + 2x + 1)(x^4 + x^3 + x^2 + 1)(x^4 + x^3 + 2x^2 + 2x + 2)(x^2 + 2x + 2)(x + 1).$$

The methods of Sec. 4 are applied as follows: First note that $h(T)(x)$ is the trace function from GF(3^4) onto GF(3); consequently all the roots of $h(T)(x) + 1$ lie in GF(3^4). Now

$$\begin{aligned} (h(x), x^4 - 1) &= h(x) \quad \text{(degree 3)}, \\ (h(x), x^2 - 1) &= x + 1 \quad \text{(degree 1)}, \\ (h(x), x - 1) &= 1 \quad \text{(degree 0)}. \end{aligned}$$

Thus we have $M_4=3^3$, $M_3=0$, $M_2=3^1$, and $M_1=3^0=1$. Then

$$R_1=M_1=1,$$

$$R_2=\mu(1)M_2+\mu(2)M_1=3-1=2,$$

$$R_3=0,$$

$$R_4=\mu(1)M_4+\mu(2)M_2+\mu(4)M_1=27-3=24.$$

Hence the number of factors of degree 1 is $1\cdot 1/1=1$, of degree 2 is $1\cdot 2/2=1$, and of degree 4 is $1\cdot 24/4=6$.

We now turn to the classification given by Ore. We have

$$f(x)=g_1(x)d_1(x)=(x-1)\cdot 1,$$

$$h(x)=g_2(x)d_2(x)=(x+1)(x^2+1)\cdot 1$$

where $d_1(x)=d_2(x)=1$. The possible values for

$$t(x)=\frac{g_2(x)}{r(x)}f(x) \qquad (r(x)|\, g_2(x))$$

are

$$r(x)=1, \qquad t_1(x)=(x-1)(x+1)(x^2+1); \tag{5.2}$$

$$r(x)=x+1, \qquad t_2(x)=(x-1)(x^2+1); \tag{5.3}$$

$$r(x)=x^2+1, \qquad t_3(x)=(x-1)(x+1); \tag{5.4}$$

$$r(x)=(x+1)(x^2+1), \qquad t_4(x)=x-1. \tag{5.5}$$

Now the index of $t(T)(x)$ is the least integer k such that $t(x)|x^k-1$. In this case, we find that the index of $t_1(T)(x)$ is 4, of $t_2(T)(x)$ is 4, of $t_3(T)(x)$ is 2, and of $t_4(T)(x)$ is 1. By direct calculation, we find that the irreducible polynomials belonging to $t_1(T)(x)$ are $x^4+x^3+x^2+x+1$, $x^4+x^3+x^2+2x+2$, x^4+x^3+2, and x^4+x^3+2x+1; those belonging to $t_2(T)(x)$ are $x^4+x^3+x^2+1$ and $x^4+x^3+2x^2+2x+2$; that belonging to $t_3(T)(x)$ is x^2+2x+2; and that belonging to $t_4(T)(x)$ is $x+1$.

Of course, to obtain the number of irreducible polynomials belonging to $t(T)(x)$, it is not actually necessary to produce them. Thus, the count given

by Ore (Theorem 2.4) for the number of polynomials belonging to $t_1(T)(x)$ is

$$\begin{aligned}\frac{n}{N}q^{d_2}\Phi\big(\bar{d}(x)\big) &= \tfrac{1}{4}\cdot 3^0\Phi(x^3+x^2+x+1)\\ &= \tfrac{1}{4}\Phi\big((x^2+1)(x+1)\big)\\ &= \tfrac{1}{4}\left[3^3\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{3^1}\right)\right]\\ &= 4.\end{aligned}$$

Similarly, the number of irreducible polynomials belonging to $t_2(T)(x)$ is $\frac{1}{4}\cdot 3^0\Phi(x^2+1)=2$, the number belonging to $t_3(T)(x)$ is 1, and the number belonging to $t_4(T)(x)$ is 1.

The next two examples illustrate the relative ease with which our method predicts the character of the factorization of $Q(h(T)(x))$.

EXAMPLE 5.2. Let $Q(x)=x^2+x+1$, the irreducible of degree 2 over GF (2). Let $h(x)=x^4+x^2+1$. In GF (2^2) we have the factorization

$$Q(h(T)(x)) = \prod_{j=0}^{1}\left[h(T)(x)-\alpha^{2^j}\right],$$

where $\deg\alpha=2$. We note that $\big(h(x),x^2-1\big)=1$, so that $d(x)=1$ and $\bar{d}(x)=x^2-1$ in Theorem 4.1. We find that $Q(x)|\bar{d}(T)(x)$. Thus for $j=0,1$, $h(T)(x)-\alpha^{2^j}$ has a root in GF (2^2) by Theorem 4.1. By Corollary 4.1, the number of roots of $h(T)(x)-\alpha^{2^j}$ of degree 2 over GF (2) is $M_2=2^0=1$ for each value of j.

We next check for additional roots in GF (2^4). [We know the roots in GF (2^2) are contained in GF (2^4).] Now $\big(h(x),x^4-1\big)=1$, and thus $M_4=2^0=1$, the number of roots of $h(T)(x)-\alpha^{2^j}$ of degree dividing 4. But we have already determined that this root has degree 2; hence there are no roots of degree 4.

We seek now the roots of degree dividing 6, i.e., the roots in GF (2^6). We have $\big(h(x),x^6-1\big)=h(x)$. Since the degree of $h(x)$ is 4, we find that $M_6=2^4=16$. This means that in GF (2^6), each $h(T)(x)-\alpha^{2^j}$ $(j=0,1)$ has 16 roots. Thus we have a total of 32 roots in GF (2^6). Since $Q(h(T)(x))$ has degree 32, we have located all the roots. Note that there are $2(16-1)=30$

roots of degree 6. Thus in the factorization of $Q(h(T)(x))$ over GF (2) we have one irreducible of degree 2 and 5 irreducibles of degree 6.

Beard [1] has found that

$$Q(h(T)(x)) = (x^2+x+1)(x^6+x^5+1)(x^6+x^5+x^2+x+1)$$
$$(x^6+x^5+x^3+x^2+1)(x^6+x^5+x^4+x+1)(x^6+x^5+x^4+x^2+1).$$

EXAMPLE 5.3. Let $Q(x)=x^3+x^2+1$, an irreducible of degree 3 over GF (2). Let $h(x)=x^3+x+1$. In GF (2^3) we have the factorization

$$Q(h(T)(x)) = \prod_{j=0}^{2} \left[h(T)(x) - \alpha^{2^j} \right],$$

where $\deg\alpha=3$. In Theorem 4.1, $\left(h(x), x^3-1\right)=1$, $d(x)=1$, and $\bar{d}(x)=x^3-1$. We note that $Q(x)|\bar{d}(T)(x)$. Thus for $j=0,1,2$, $h(T)(x)-\alpha^{2^j}$ has $M_3=2^0=1$ root of degree 3 over GF (2), for a total of 3 roots of degree 3 over GF (2). For $i=2,3,4,5,6$ we calculate that $\left(h(x), x^{3^i}-1\right)=1$ and thus $M_{3^i}=1$. Hence no additional roots are obtained in the GF (2^{3^i}), $i=2,3,4,5,6$. However, for $i=7$, $\left(h(x), x^{3^i}-1\right)=\left(h(x), x^{21}-1\right)=h(x)$. By Corollary 4.1 the number of roots of each $h(T)(x)-\alpha^{2^j}$ is $M_{21}=2^3=8$, for a total of 24 roots. Since the degree of $Q(h(T)(x))$ is 24, we have obtained all roots. The additional $24-3=21$ roots counted in M_{21} all have degree 21 over GF (2). Thus $Q(h(T)(x))$ is the product over GF (2) of one irreducible of degree 3 and one irreducible of degree 21. Beard [1] has computed

$$Q(h(T)(x))$$
$$=(x^3+x^2+1)(x^{21}+x^{20}+x^{19}+x^{17}+x^{15}+x^{14}+x^{12}+x^7+x^6+x^5+1).$$

AUTHOR'S NOTE

Due to a clerical error, the authors' second paper on this subject, "Factorization of $Q(h(T)(x))$ over a finite field, where $Q(x)$ is irreducible and $h(T)(x)$ is linear—II" has already appeared [*LAA*, Vol. 10 (1), 53–72 (1975)]. Because of this, we have deleted from the present paper an analysis of the substitution $Q(x^{q^r}-x)$. The more general substitution $Q(x^{p^r}-x)$ is discussed in the second paper.

REFERENCES

1 Jacob T. B. Beard, Computing in GF (q), *Math. Comput.* **28** (No. 128, Oct. 1974), 1159–1168.
2 Leonard Eugene Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.
3 Andrew F. Long, Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x, *Duke Math. J.* **40** (1973), 63–76.
4 Andrew F. Long, Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x, *Acta Arith.* **25** (1973), 65–80.
5 Oystein Ore, Contributions to the theory of finite fields, *Trans. Am. Math. Soc.* **36** (1934), 243–274.
6 Theresa P. Vaughan, Polynomials and linear transformations over finite fields, *J. Reine Ange. Math.* **267** (1974), 179–206.

Received 13 March 1975; revised 28 July 1975